

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-187836

(43)Date of publication of application : 21.07.1998

(51)Int.Cl.

G06F 17/60

G09C 1/00

(21)Application number : 09-292921

(71)Applicant : FUJITSU LTD

(22)Date of filing : 24.10.1997

(72)Inventor : KURODA YASUTSUGU

KOMURA MASAHIRO

TORII SATORU

IWASE SHIYOUKO

ONO KOSHIO

(30)Priority

Priority number : 08288539

Priority date : 30.10.1996

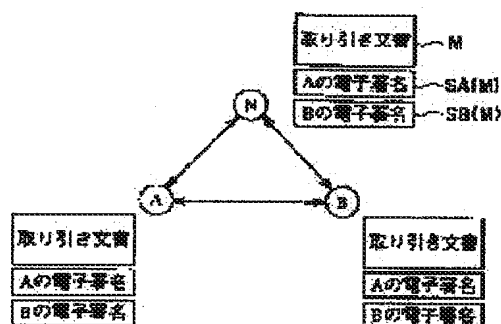
Priority country : JP

(54) DEVICE AND METHOD FOR PROVING TRANSACTION IN NETWORK ENVIRONMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To guarantee the safety of transaction to be performed between users while utilizing a communication network.

SOLUTION: A transaction document M describing the contents of transaction between users A and B is prepared and an electronic signature SA(M) of user A and an electronic signature SB(M) of user B for that document are prepared. Then, these signatures are sent to the notarial act equipment of notarial person N together with the transaction document M and the users A and B and the notarial person N share information. Thus, the notarial person N can objectively prove the contents, etc., of transaction.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(1) 特許出願番号

特開平10-187⁸³6

(43)公開日 平成10年(1998)7月21日

(5) Int. Cl.⁵
G 0 6 F 17/60

記号

G 0 9 C 1/00

6 6 0

F I
G 0 6 F 1 5/21

3 0
3

G 0 9 C 1/00

6 6 0 B、

審査請求 未請求 請求項の数25 O L (全 26 頁)

(21)出願番号 特願平9-292921

(22)出願日 平成9年(1997)10月24日

(31)優先権主張番号 特願平8-288539

(32)優先日 平8(1996)10月30日

(33)優先権主張国 日本 (J P)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 黒田 康嗣

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 小村 昌弘

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 弁理士 大曾 義之 (外1名)

最終頁に続く

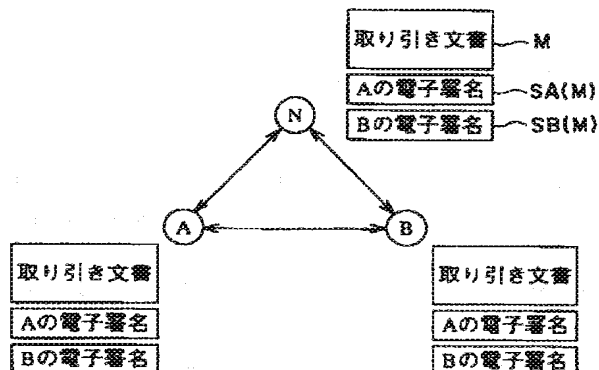
(54)【発明の名称】 ネットワーク環境における取り引き証明装置および方法

(57)【要約】

【課題】 ユーザ間で行われる取り引きの安全性を、通信ネットワークを利用して保証することが課題である。

【解決手段】 ユーザAとユーザBの取り引きの内容を記述した取り引き文書Mを作成し、それに対するユーザAの電子署名SA(M)およびユーザBの電子署名SB(M)を作成する。そして、それらを取り引き文書Mとともに公証人Nの公証装置に送り、ユーザA、B、および公証人Nが情報を共有する。こうして、第3者である公証人Nが、取り引きの内容等を客観的に証明することができる。

内容保証サービスにおける共有情報を示す図



【特許請求の範囲】

【請求項1】 複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、通信ネットワークに接続され、第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データと第2のユーザの電子署名データとを、該ネットワークから受け取る通信手段と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを検証する処理手段と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項2】 前記通信手段は、前記ネットワークから前記取り引き文書データをさらに受け取り、前記処理手段は、該取り引き文書データを用いて前記第1のユーザの電子署名データと第2のユーザの電子署名データを検証し、該取り引き文書データを、該第1のユーザの電子署名データと第2のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項1記載の取り引き証明装置。

【請求項3】 取り引き日時を表す日時情報を発行する日時発行手段をさらに備え、前記通信手段は、日時情報を含む前記取り引き文書データを受け取り、前記処理手段は、該取り引き文書データに含まれる日時情報が前記日時発行手段が発行した日時情報と一致するかどうかを確認することを特徴とする請求項2記載の取り引き証明装置。

【請求項4】 取り引きの識別子情報を発行する識別子発行手段をさらに備え、前記通信手段は、識別子情報を含む前記取り引き文書データを受け取り、前記処理手段は、該取り引き文書データに含まれる識別子情報が前記識別子発行手段が発行した識別子情報と一致するかどうかを確認することを特徴とする請求項2記載の取り引き証明装置。

【請求項5】 前記記憶手段は、前記第1のユーザおよび第2のユーザが保存している第1のユーザの電子署名データ、第2のユーザの電子署名データ、および取り引き文書データと共通の前記第1のユーザの電子署名データ、第2のユーザの電子署名データ、および取り引き文書データを記憶することを特徴とする請求項2記載の取り引き証明装置。

【請求項6】 前記通信手段は、前記ネットワークから前記取り引き文書データの参照要求を受け取り、前記処理手段は、該参照要求に応じて該取り引き文書データを前記記憶手段から取り出し、該通信手段は、該取り引き文書データの内容を、該ネットワークを介して要求元に送ることを特徴とする請求項2記載の取り引き証明装置。

【請求項7】 前記処理手段は、前記第1のユーザの電

子署名データと第2のユーザの電子署名データの少なくとも一方を含むデータに第3者の電子署名を施し、第3者の電子署名データを生成して、該第3者の電子署名データを前記記憶手段に格納することを特徴とする請求項1記載の取り引き証明装置。

【請求項8】 前記通信手段は、前記第3者の電子署名データを、前記ネットワークを介して前記第1のユーザおよび第2のユーザに送ることを特徴とする請求項7記載の取り引き証明装置。

10 【請求項9】 前記通信手段は、前記ネットワークから前記取り引き文書データに対する合意者の電子署名をさらに受け取り、該合意者の電子署名を前記第1のユーザの電子署名データと第2のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項1記載の取り引き証明装置。

【請求項10】 前記通信手段は、暗号化された前記第1のユーザの電子署名データと第2のユーザの電子署名データとを受け取り、前記処理手段は、該暗号化された第1のユーザの電子署名データと第2のユーザの電子署名データを復号化してから検証することを特徴とする請求項1記載の取り引き証明装置。

【請求項11】 複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、通信ネットワークに接続され、第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データに対して作成された第2のユーザの電子署名データを、該ネットワークから受け取る通信手段と、

前記第2のユーザの電子署名データを検証する処理手段と、
前記第2のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項12】 複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、通信ネットワークに接続され、第1のユーザと第2のユーザの間の取り引きに関する事項を記述した第1のユーザの取り引き情報と第2のユーザの取り引き情報とを、該ネットワークから受け取る通信手段と、
前記第1のユーザの取り引き情報と第2のユーザの取り引き情報の内容が同じであることを確認する処理手段と、
前記取り引き情報を記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項13】 複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データを作成する処理手段と、
通信ネットワークに接続され、前記第1のユーザの電子署名データを該ネットワークを介して第3者に送信し、

前記取り引き文書データに対する第2のユーザの電子署名データであって、該第3者により検証された該第2のユーザの電子署名データを、該第3者から該ネットワークを介して受信する通信手段と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項14】 前記通信手段は、前記第3者に前記ネットワークを介して前記取り引き文書データをさらに送信し、前記第3者により該取り引き文書データを用いて検証された前記第2のユーザの電子署名データを受信し、該取り引き文書データを、前記第1のユーザの電子署名データと第2のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項13記載の端末装置。

【請求項15】 複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データを作成する処理手段と、

通信ネットワークに接続され、前記取り引き文書データに対する第2のユーザの電子署名データを前記第2のユーザから該ネットワークを介して受信し、前記第1のユーザの電子署名データと第2のユーザの電子署名データを、該ネットワークを介して第3者に送信する通信手段と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項16】 前記通信手段は、前記第1のユーザの電子署名データと第2のユーザの電子署名データの少なくとも一方を含むデータに対する前記第3者の電子署名データを、前記ネットワークから受信し、前記処理手段は、該第3者の電子署名データを検証して前記記憶手段に格納することを特徴とする請求項13または15記載の端末装置。

【請求項17】 複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した第1のユーザの取り引き情報を作成する処理手段と、

通信ネットワークに接続され、前記第1のユーザの取り引き情報を該ネットワークを介して第3者に送信し、該第3者により第2のユーザの取り引き情報と内容が同じであることを確認された該第1のユーザの取り引き情報を、該第3者から該ネットワークを介して受信する通信手段と、

受信した取り引き情報を記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項18】 複数のユーザ間で行われる取り引きに

関する情報処理を行う端末装置であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した第1のユーザの取り引き情報を作成する処理手段と、

通信ネットワークに接続され、前記第2のユーザの取り引き情報を前記第2のユーザから該ネットワークを介して受信し、前記第1のユーザの取り引き情報と第2のユーザの取り引き情報を、該ネットワークを介して第3者に送信する通信手段と、

10 前記第1のユーザの取り引き情報を記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項19】 複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明システムであって、第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データを作成する作成手段と、

前記取り引き文書データに対する第2のユーザの電子署名データを作成する作成手段と、

20 通信ネットワークに接続され、前記第1のユーザの電子署名データと第2のユーザの電子署名データを、該ネットワークから受け取る通信手段と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを検証する処理手段と、

前記第1のユーザにより参照され、前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する第1の記憶手段と、

前記第2のユーザにより参照され、前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する第2の記憶手段と、

30 第3者により参照され、前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する第3の記憶手段と

を備えることを特徴とする取り引き証明システム。

【請求項20】 前記第1のユーザの電子署名データと第2のユーザの電子署名データの少なくとも一方を含むデータに対する前記第3者の電子署名データを作成する作成手段をさらに備え、前記処理手段は、該第3者の電子署名データを検証し、前記第1、第2、および第3の記憶手段は、該第3者の電子署名データをさらに記憶すること

40 を特徴とする請求項19記載の取り引き証明システム。

【請求項21】 複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データと第2のユーザの電子署名データと

を、通信ネットワークから受け取る機能と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを検証する機能と、

50

前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項22】 複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データを作成する機能と、

前記第1のユーザの電子署名データを通信ネットワークを介して第3者に送信し、前記取り引き文書データに対する第2のユーザの電子署名データであって、該第3者により検証された該第2のユーザの電子署名データを、該第3者から該ネットワークを介して受信する機能と、前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項23】 複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第1のユーザの電子署名データを作成する機能と、

前記取り引き文書データに対する第2のユーザの電子署名データを前記第2のユーザから通信ネットワークを介して受信し、前記第1のユーザの電子署名データと第2のユーザの電子署名データを、該ネットワークを介して第3者に送信する機能と、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを記憶する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項24】 複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明方法であって、

第1のユーザと第2のユーザの間の取り引きに関する事項を記述した取り引き文書データを作成し、

前記取り引き文書データに対する第1のユーザの電子署名データと第2のユーザの電子署名データを作成し、

前記第1のユーザの電子署名データと第2のユーザの電子署名データとを、通信ネットワークを介して第3者に送信し、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを検証し、

前記第1のユーザの電子署名データと第2のユーザの電子署名データを保存することを特徴とする取り引き証明方法。

【請求項25】 前記第1のユーザの電子署名データと第2のユーザの電子署名データの少なくとも一方を含む

データに対する前記第3者の電子署名データを作成し、該第3者の電子署名データを検証し、該第3者の電子署名データを保存することを特徴とする請求項24記載の取り引き証明方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、2以上の当事者間で行われる取り引きの内容等の取り引きに関する事項を、通信ネットワークを利用して客観的に証明する取り引き証明装置およびその方法に関する。

【0002】

【従来の技術】今日、インターネットやパーソナルコンピュータの普及に伴い、通信ネットワークを介してコンピュータ間で様々な取り引きが行われつつある。しかし、インターネットには基本的に誰でも自由にアクセスすることができるため、通信相手の本人確認が難しく、送信データが盗用されたり、改ざんされたりする恐れもある。

【0003】このため、ネットワーク環境において本格的な商取引を行うには、このような不正行為を防止する工夫が必要不可欠となる。従来の不正行為防止方法には、例えば次のようなものがある。

(a) 電子取引方式(特開昭62-056043)

署名者が自分の電子署名(電子捺印)を作成する際、認証用データの定まった位置に電子署名の猶予期限を示す日付データを付加する。これにより、電子署名を受信した認証者に対して応答の期限を明示し、期限までに応答がない場合、取り引きが中止となり、送信した電子署名が無効になることを宣言する。

【0004】署名者は、猶予期限を過ぎても応答が得られない場合、その事実を電子署名とともに公証機関に届けることによって電子署名を無効にできるようにする。これにより、電子署名の認証者が応答を返さずに持ち逃げした場合や認証者が不正な署名を送信した場合でも、電子署名の悪用を防止できる。

(b) 電子的公証方法および装置(特開平06-014018)

データが真正であることの証明を希望する当事者からデータが電子的公証装置に供給されると、日時発生器は、当事者が変更できないある時点を指定する日時情報を発生する。そして、データの内容と日時情報が暗号器により暗号化され、日時が印字された真正証明データが公証装置から出力される。これにより、文書または電子的に記録されたデータが、印字された日時以降変更されなかったことが確認でき、文書の真正性を電子的に公証することができる。

【0005】

【発明が解決しようとする課題】しかしながら、上述のような従来の不正行為防止方法には次のような問題がある。

【0006】電子取引方式によれば、電子署名の有効期限を取り引き相手に通知して、その悪用を防止することができる。しかし、これにより、取り引き相手の確認を行ったり、取り引き内容の改ざんを防止したりすることはできない。

【0007】また、電子的公証方法によれば、公証装置が文書に日時情報を付加することで、その真正性を電子的に公証することができる。しかし、この公証装置は、単独の当事者が入力したデータの真正性を証明するため、入力前にデータが改ざんされたかどうかは判定することができない。したがって、2者間の取り引き文書等の場合、結果的に不正な内容が真正データとして出力される可能性がある。

【0008】したがって、悪意のあるユーザが取り引き内容等を偽る可能性があり、ネットワークを利用した商取引が必ずしも安全に行われるとは限らないという問題がある。

【0009】ところで、商品取引所における取引の管理形態は次のようなものである。先物売買などの商品の取引は、すべて商品取引所で行われる。取引の当事者は取引所の会員となり、あらかじめ一定金額の保証金を収めておく。そして、不正が行われた場合には、保証金が没収される。

【0010】しかしながら、商品取引所における取引は、一般的な企業間取引とは異なっており、ネットワーク上の商取引にそのまま応用するのは困難である。

【0011】本発明の課題は、2以上の当事者間で行われる取引の安全性を、通信ネットワークを利用して保証する取引証明装置およびその方法を提供することである。

【0012】

【課題を解決するための手段】図1は、本発明の取引証明システムの原理図である。図1の取引証明システムは、取引証明装置1、第1のユーザの端末装置2、および第2のユーザの端末装置3を含み、複数のユーザ間で行われる取引に関する情報処理を行う。取引証明装置1と端末装置2、3は、通信ネットワーク4により互いに結合されている。

【0013】端末装置2は、第1のユーザと第2のユーザの間の取引に関する事項を記述した取引文書データに対する第1のユーザの電子署名データ8を作成し、端末装置3は、その取引文書データに対する第2のユーザの電子署名データ9を作成する。これらの電子署名データ8、9は、ネットワーク4を介して、取引証明装置1に送信される。

【0014】取引証明装置1は第3者の情報処理装置に相当し、通信手段5、処理手段6、および記憶手段7を備える。通信手段5は、ネットワーク4に接続され、第1のユーザの電子署名データ8と第2のユーザの

電子署名データ9とをネットワーク4から受け取る。

【0015】処理手段6は、第1のユーザの電子署名データ8と第2のユーザの電子署名データ9を検証し、記憶手段7は、第1のユーザの電子署名データ8と第2のユーザの電子署名データ9を記憶する。

【0016】電子署名とは、データの送信者が本人しか知らない秘密鍵を用いて、なんらかの方法でデータを暗号化して作成した情報である。ここでは、第1のユーザの電子署名データ8は、第1のユーザの秘密鍵を用いて作成され、第2のユーザの電子署名データ9は、第2のユーザの秘密鍵を用いて作成される。

【0017】ユーザの電子署名は、そのユーザ自身しか作成できないので、取引文書データにユーザの電子署名が施されると、取引内容がそのユーザにより承認されたものとみなされる。

【0018】処理手段6は、通信手段5を介してこれらの電子署名データ8、9を受け取ると、第1のユーザの公開鍵、第2のユーザの公開鍵を用いて電子署名データ8、9をそれぞれ復号化し、それらの内容を検証する。

【0019】両者の内容が同じであれば、第1および第2のユーザの双方が取引に合意したものとみなし、その証拠として電子署名データ8、9を記憶手段7に保存する。もし両者の内容が異なれば、その取引は不成立とみなして、端末装置2、3にエラー通知を行う。

【0020】このように、取引の当事者とは異なる第3者の取引証明装置1が電子署名データ8、9を保管しておけば、取引が成立していることとその内容等を、いつでも他人に対して証明することが可能になる。したがって、取引の当事者である第1および第2のユーザは、取引に関する事項を偽ることが不可能になり、ネットワーク環境における取引の安全性が客観的に保証される。

【0021】例えば、図1の取引証明装置1は、実施形態の図3における公証装置11に対応し、通信手段5は図4におけるネットワーク接続装置27に対応し、処理手段6はCPU21（中央処理装置）とメモリ22に対応し、記憶手段7はメモリ22または外部記憶装置25に対応する。

【0022】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。商取引は、一般的に2人の当事者間の同意のもとに成り立つ。しかし、当事者同士が同意したことを客観的に証明するためには、“信頼のおける第三者（trusted third party）”が必要である。なぜなら、2者間のみの取引では、一方がその事実を偽ることができるからである。

【0023】本実施形態では、この“信頼のおける第三者”を“公証人（notary public）”または“notarization authority”と呼び、公証人がネットワーク環境での商取引を安全に行うことを保証する取引証明

システムを、取り引き公証システムと呼ぶことにする。

【0024】ネットワーク環境で安全な商取り引きを行うには、取り引き公証システムが以下のようなサービスを提供する必要がある。

(1) 身元保証サービス

公証人が、取り引きする相手の身元を保証する。これにより、偽りの取り引き相手を検出できる。

(2) 日時保証サービス

公証人が、取り引きした日時を保証する。これにより、取り引きした日時を偽れなくなる。

(3) 一意性保証サービス

公証人が、取り引きの一意性を保証する。これにより、他の取り引きとの混同が防止される。

(4) 配達保証サービス

公証人が、取り引き情報が確実に配送されたことを保証する。これにより、取り引き情報の発信人が情報を発信したことを偽れなくなり、取り引き情報の受信人も情報を受信したことを偽れなくなる。また、取り引き情報が配送されなかった場合、どこで配送されなかったのかを検出できる。

(5) 内容保証サービス

公証人が、取り引きの内容を保証する。これにより、内容が改ざんされたことを検出できる。また、必要に応じて、いつでも取り引き内容を参照できる。

(6) 取り引き保証サービス

公証人が、特定の当事者同士が取り引きしたことを保証する。これにより、当事者が、取り引きしたことを偽れなくなる。

【0025】図2は、ネットワーク上での2者間の商取り引き環境を示している。図2において、例えば、当事者Aは取り引き情報の第1発信者であり、当事者Bはその取り引き情報の受信者である。当事者A、Bは、互いにインターネット等の通信ネットワークを使って売買契約書等の取り引き情報を交換し、商取り引きを行っている。公証人Nは、当事者A、Bとの間で個別に取り引き情報を交換して、それらを確認し、取り引きの安全性を保証する。

【0026】図3は、図2のような商取り引き環境を実現するための取り引き公証システムの構成図である。図3の取り引き公証システムは、公証人Nの情報処理装置である公証装置11、ユーザA、B、C、D、・・・の計算機端末12A、12B、12C、12D、・・・を備える。公証装置11および端末12A、12B、12C、12D、・・・は、通信ネットワーク13を介して互いに結合されている。

【0027】図4は、公証装置11およびユーザ端末12A、12B、12C、12Dとして用いられる情報処理装置の構成図である。図4の情報処理装置は、CPU21、メモリ22、入力装置23、出力装置24、外部記憶装置25、媒体駆動装置26、ネットワーク接続装

置27を備え、それらの各装置はバス28により互いに結合されている。

【0028】CPU21は、メモリ22を利用しながらプログラムを実行して、上述の各サービスを実現する。メモリ22としては、例えばROM (read only memory)、RAM (random access memory) 等が用いられる。メモリ22には、上述のプログラムと、処理に必要なデータが格納される。

【0029】入力装置22は、例えばキーボード、ポインティングデバイス等に相当し、ユーザからの要求や指示の入力に用いられる。また、出力装置24は、表示装置やプリンタ等に相当し、取り引き情報等の出力に用いられる。

【0030】外部記憶装置25は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置25に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ22にロードして使用することができる。また、外部記憶装置25は、取り引き情報を保存するデータベースとしても使用される。

【0031】媒体駆動装置26は、可搬記録媒体29を駆動し、その記憶内容にアクセスすることができる。可搬記録媒体29としては、メモ리카ード、フロッピーディスク、CD-ROM (compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体29に、上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ22にロードして使用することができる。

【0032】ネットワーク接続装置27は、通信ネットワーク13に接続され、通信に伴うデータ変換等を行う。情報処理装置は、ネットワーク接続装置27を介して、取り引き情報等を送受信することができる。また、情報処理装置は、必要に応じて、外部の情報提供者のデータベース30等と通信して、データベース30から上述のプログラムとデータを受け取り、それらをメモリ22にロードして使用することができる。

【0033】ところで、上述のサービスのうち、身元保証サービスは、今日の社会における印鑑証明サービスに相当する。印鑑証明サービスは、取り引きの当事者の身元が確かなことを保証するサービスである。当事者は役所に印鑑を登録しておき、取り引き文書にその印鑑で朱印を押すことで自分の身元を証明する。

【0034】このサービスをネットワーク上で実現するために、公証人Nが電子署名の正当性を証明する。電子署名とは、データの送信者が本人しか知らない秘密鍵を用いて、なんらかの方法でデータを暗号化して作成した情報である。この情報は、本人しか生成することができないので、ネットワーク環境では印鑑の印影と同様の役割を果たす。

【0035】具体的には、ITU (International Telecommunication Union) X. 509で勧告されている認証局の枠組を利用することができる。この枠組によれば、当事者の身元が確かであることを確認するためには、認証局から発行される証明書の中の公開鍵を用いて電子署名を復号化し、その内容を検証すればよい。電子署名の生成に用いられる秘密鍵と証明書に記載される公開鍵とは対になっており、秘密鍵により暗号化されたデータは公開鍵により復号化することができる。

【0036】また、公証人Nは、取り引きした日付けや時刻を表す日時情報を当事者に発行することで、日時保証サービスを提供する。これにより、取り引きした日時を保証し、同じ当事者間の過去の取り引き内容との混同を避けることができる。

【0037】さらに、公証人Nは、取り引きの識別子としてトランザクションIDを当事者に発行することで、一意性保証サービスを提供する。これにより、各取り引きが正しく識別され、他の取り引き内容との混同を避けることができる。

【0038】また、配達保証サービスは、ISO (International Standardization Organization) / IEC (International Electrotechnical Commission) CID 13888-1, 2, 3により標準化されている否認拒否機構 (non-repudiation mechanism) を用いて実現することができる。この否認拒否機構は、配達の出発となるトークン情報を発行し、ユーザの要求に応じてそれを確認することで、メッセージが配達されたことを証明する。以下では、この配達保証サービスについては詳述を避けることにする。

【0039】次に、図5から図10までを参照しながら、内容保証サービスの実施形態について説明する。2人の当事者間でやりとりされる取り引き情報の内容を保証するには、以下のようなサービス要件が考えられる。

【1】取り引き内容を発信者が確認したことを保証するために、取り引き内容に発信者の電子署名を付加する。

【2】取り引き内容を受信者が確認したことを保証するために、取り引き内容に受信者の電子署名を付加する。

【3】最終的に発信者および受信者が取り引き内容を確認したことを保証するために、発信者および受信者の電子署名が付いた取り引き情報を、発信者、受信者、および公証人Nが共有する。

【4】取り引き内容をいつでも参照できることを保証するために、公証人Nが取り引き内容を蓄積する。

【0040】以上の要件を満たすためには、発信者と受信者の電子署名が付いた取り引き情報を、発信者、受信者、および公証人Nが共有する必要がある。図5においては、取り引き内容が記述された取り引き文書Mと、それに対するユーザAの電子署名SA(M)と、ユーザBの電子署名SB(M)とが、ユーザA、B、および公証人Nにより共有されている。

【0041】図6は、図5の取り引き文書Mの一例を示している。図6の取り引き文書Mの中には、売買の当事者、売買の対象、売買金額、売買日時等の取り引き内容を記述した平文Pのほかに、公証人Nが発行する日時情報TとトランザクションIDが含まれている。ここでは、“19960808142356”が日時情報Tに相当し、“1996年8月8日14時23分56秒”を表している。また、“4567”は、トランザクションIDが“0x4567(16進数)”であることを表している。

【0042】Nの電子署名SN(T, ID)は、日時情報TとトランザクションIDを連結したデータに対する公証人Nの電子署名を表す。このSN(T, ID)の代わりに、日時情報Tのみに対する公証人Nの電子署名SN(T)とトランザクションIDのみに対する公証人Nの電子署名SN(ID)を付加してもよい。

【0043】このような内容保証サービスの実施形態としては、図7、8、9、10に示すような4つの基本モデルが考えられる。これらのモデルにおいては、図6のような取り引き文書Mが用いられ、ユーザA、B、および公証人Nの間でやりとりされる情報には発信者の電子署名が付いている。受信者はその電子署名を検証することで、発信者の身元を確認することができる。したがって、これらのモデルは、身元保証サービス、日時保証サービス、および一意性保証サービスを含んでいる。

【0044】図7は、内容保証サービスの第1のモデルを示している。第1のモデルでは、ユーザA、Bがオンラインまたはオフラインで取り引き内容Pを交換した後、それぞれが公証装置11に対して取り引き情報を送付する。図7における処理の流れは、次のようになる。

【0045】P0: ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P0': ユーザBの端末12Bが、公証装置11から日時情報TとトランザクションIDを取得する。

【0046】処理P0およびP0'において、公証装置11は、取り引きの当事者であるユーザAとユーザBに、同一の日時情報TとトランザクションIDを発行する。

P1: 端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を公証装置11に送信する。

【0047】電子署名SA(M)の作成方法としては、任意のものをを用いることができる。例えば、取り引き文書Mを所定の圧縮アルゴリズムで圧縮したり、ハッシュしたりしてデータ量を削減し、得られたデータを秘密鍵SAで暗号化する方法がある。もちろん、取り引き文書

Mをそのまま秘密鍵SAで暗号化してもかまわない。

【0048】P1' : 端末12Bが、日時情報TとトランザクションIDと取引引き内容Pを連結して、取引引き文書M'を作成する。次に、ユーザBの秘密鍵SBを取り出し、それを用いて取引引き文書M'に対する電子署名SB(M')を作成する。そして、データ{M', SB(M')}を公証装置11に送信する。

【0049】P2 : 公証装置11が、データ{M, SA(M)}とデータ{M', SB(M')}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M')を検証する。

【0050】例えば、圧縮処理やハッシュ処理により、電子署名SA(M)、SB(M')の中の取引引き文書M、M'のデータ量が削減されている場合は、公証装置11は、受け取った取引引き文書M、M'に同様のデータ削減処理を施す。そして、得られたデータと、SA(M)、SB(M')を公開鍵PA、PBで復号化したデータとを、それぞれ比較して、SA(M)、SB(M')の正当性を検証する。

【0051】もし、圧縮処理やハッシュ処理が行われていない場合は、受け取った取引引き文書M、M'を、そのまま、SA(M)、SB(M')を復号化したデータと比較するだけでよい。ここで、SA(M)またはSB(M')が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

【0052】次に、公証装置11は、取引引き文書MとM'が同一かどうかを確認する。具体的には、これらの取引引き文書に記述された日時情報T、トランザクションID、取引引き内容Pをそれぞれ比較し、両者が一致することを確認する。また、取引引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。

【0053】取引引き文書MとM'が一致しない場合、あるいは、日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0054】次に、公証装置11は、取引引き文書M、電子署名SA(M)、SB(M')を連結して、データ{M, SA(M), SB(M')}を作成し、それを保

存する。

【0055】P3 : 公証装置11が、データ{M, SA(M), SB(M')}を端末12Aに送信する。

【0056】P4 : 端末12Aが、データ{M, SA(M), SB(M')}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M')を検証する。ここで、SA(M)またはSB(M')が正しくな

ければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。

【0057】次に、端末12Aは、公証装置11から受け取った取引引き文書Mと端末12Aが作成した取引引き文書Mが同一かどうかを確認する。受け取った取引引き文書Mが正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それが正しければ、データ{M, SA(M), SB(M')}を保存して、処理を終了する。

【0058】P4' : 端末12Bが、データ{M, SA(M), SB(M')}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M')を検証する。ここで、SA(M)またはSB(M')が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0059】次に、端末12Bは、公証装置11から受け取った取引引き文書M'と端末12Bが作成した取引引き文書M'が同一かどうかを確認する。受け取った取引引き文書M'が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。それが正しければ、データ{M, SA(M), SB(M')}を保存して、処理を終了する。

【0060】このような第1のモデルでは、ユーザA、Bの双方が独立に取引引き情報を公証人Nに送付するため、ユーザAとユーザBが対等な立場にあるといえる。また、ユーザA、Bは、各自の電子署名を付けるだけでサービスを受けることができる。一方、公証装置11は、ユーザA、Bの電子署名の検証の他に、取引引き文書MとM'の同一性の検証を行わなければならない。

【0061】ただし、このモデルでは、公証装置11が取引引き文書M、M'の同一性の検証に失敗した場合、ユーザA、Bのどちらが内容を改ざんしたのかを特定できない。また、ユーザAとユーザBの公証装置11に対する取引引き情報の送付がタイミングよく行われず、公証装置11がそれらを検証できない可能性もある。

【0062】図8は、内容保証サービスの第2のモデルを示している。第2のモデルでは、ユーザA、Bがオンラインまたはオフラインで取引引き内容Pを交換した後、ユーザAのみが公証装置11に対して取引引き情報を送付する。図8における処理の流れは、次のようになる。

【0063】P10 : ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P11 : 端末12Aが、日時情報TとトランザクションIDと取引引き内容Pを連結して、取引引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取引引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を端末1

2 Bに送信する。

【0064】P12: 端末12 Bが、データ {M, SA (M)} を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA (M) を検証する。ここで、SA (M) が正しくなければ、公証装置11、端末12 Aにエラー通知を行って処理を終了する。

【0065】次に、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB (M) を作成する。そして、データ {M, SA (M), SB (M)} を作成して、それを保存する。

【0066】P13: 端末12 Bが、データ {M, SA (M), SB (M)} を端末12 Aに送信する。

P14: 端末12 Aが、データ {M, SA (M), SB (M)} を受信する。そして、ユーザBの公開鍵PBを取り出し、それを用いてSB (M) を検証する。ここで、SB (M) が正しくなければ、公証装置11、端末12 Bにエラー通知を行って処理を終了する。それが正しければ、データ {M, SA (M), SB (M)} を保存する。

【0067】P15: 端末12 Aが、データ {M, SA (M), SB (M)} を公証装置11に送信する。

P16: 公証装置11が、データ {M, SA (M), SB (M)} を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA (M) を検証し、公開鍵PBでSB (M) を検証する。ここで、SA (M) またはSB (M) が正しくなければ、端末12 A、12 Bにエラー通知を行って処理を終了する。

【0068】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12 A、12 Bにエラー通知を行って処理を終了する。

【0069】電子署名SA (M)、SB (M)、日時情報T、およびトランザクションIDが正しければ、公証装置11は、データ {M, SA (M), SB (M)} を保存して、処理を終了する。

【0070】このような第2のモデルでは、ユーザAのみが取り引き情報を公証人Nに送付するため、最終的に内容保証サービスを受けるかどうかをユーザAが決定することができる。したがって、ユーザAの方が有利な立場にあるといえる。

【0071】また、ユーザBは、取り引き文書MにユーザAの電子署名が付いた情報がないとサービスを受けられない。一方、ユーザAは、ユーザBの電子署名がないとサービスを受けられないが、過去に作成されたユーザBの電子署名付きの情報を公証人Nに送付することができる。

【0072】図9は、内容保証サービスの第3のモデルを示している。第3のモデルでは、ユーザA、Bがオンラインまたはオフラインで取り引き内容Pを交換した

後、ユーザBのみが公証装置11に対して取り引き情報を送付する。図9における処理の流れは、次のようになる。

【0073】P20: ユーザAの端末12 Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P21: 端末12 Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA (M) を作成する。そして、データ {M, SA (M)} を端末12 Bに送信する。

【0074】P22: 端末12 Bが、データ {M, SA (M)} を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA (M) を検証する。ここで、SA (M) が正しくなければ、公証装置11、端末12 Aにエラー通知を行って処理を終了する。

【0075】次に、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB (M) を作成する。そして、データ {M, SA (M), SB (M)} を作成して、それを保存する。

【0076】P23: 端末12 Bが、データ {M, SA (M), SB (M)} を公証装置11に送信する。

P24: 公証装置11が、データ {M, SA (M), SB (M)} を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA (M) を検証し、公開鍵PBでSB (M) を検証する。ここで、SA (M) またはSB (M) が正しくなければ、端末12 A、12 Bにエラー通知を行って処理を終了する。

【0077】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12 A、12 Bにエラー通知を行って処理を終了する。

【0078】電子署名SA (M)、SB (M)、日時情報T、およびトランザクションIDが正しければ、公証装置11は、データ {M, SA (M), SB (M)} を保存する。

【0079】P25: 公証装置11が、データ {M, SA (M), SB (M)} を端末12 Aに送信する。

P26: 端末12 Aが、データ {M, SA (M), SB (M)} を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA (M) を検証し、公開鍵PBでSB (M) を検証する。ここで、SA (M) またはSB (M) が正しくなければ、公証装置11、端末12 Bにエラー通知を行って処理を終了する。それらが正しければ、データ {M, SA (M), SB (M)} を保存して、処理を終了する。

【0080】このような第3のモデルでは、ユーザBのみが取り引き情報を公証人Nに送付するため、最終的に

内容保証サービスを受けるかどうかをユーザBが決定することができる。したがって、ユーザBの方が有利な立場にあるといえる。しかし、ユーザBは、取り引き文書MにユーザAの電子署名が付いた情報がないとサービスを受けられない。一方、ユーザAは、公証人Nから取り引き情報を受け取らないと、ユーザBが承認したのかどうか分からない。

【0081】図10は、内容保証サービスの第4のモデルを示している。第4のモデルでは、公証装置11がユーザAとユーザBの取り引きを仲介する。図10における処理の流れは、次のようになる。

【0082】P30：ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P31：端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を公証装置11に送信する。

【0083】P32：公証装置11が、データ{M, SA(M)}を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA(M)を検証する。ここで、SA(M)が正しくなければ、端末12Aにエラー通知を行って処理を終了する。それが正しければ、データ{M, SA(M)}を端末12Bに送信する。

【0084】P33：端末12Bが、データ{M, SA(M)}を受信する。ユーザBは、受け取った取り引き文書Mの中の取り引き内容Pを見て、その取り引きに応じられない場合は、その旨を端末12Aに通知し、端末12Bの処理を終了させる。また、その取り引きに応じる場合は、端末12Bに処理の続行を指示する。

【0085】次に、端末12Bは、ユーザAの公開鍵PAを取り出し、それを用いてSA(M)を検証する。ここで、SA(M)が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0086】次に、端末12Bは、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB(M)を作成する。そして、データ{M, SA(M), SB(M)}を作成して、それを保存する。

【0087】P34：端末12Bが、データ{M, SA(M), SB(M)}を公証装置11に送信する。

P35：公証装置11が、データ{M, SA(M), SB(M)}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証する。ここで、SA(M)またはSB(M)が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

【0088】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したも

のと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0089】電子署名SA(M)、SB(M)、日時情報T、およびトランザクションIDが正しければ、公証装置11は、データ{M, SA(M), SB(M)}を保存する。

【0090】P36：公証装置11が、データ{M, SA(M), SB(M)}を端末12Aに送信する。

P37：端末12Aが、データ{M, SA(M), SB(M)}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証する。ここで、SA(M)またはSB(M)が正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それらが正しければ、データ{M, SA(M), SB(M)}を保存して、処理を終了する。

【0091】このような第4のモデルでは、ユーザAとユーザBの取り引きを公証人Nが仲介するため、取り引き内容の改ざんが行われた場合、ユーザAとユーザBのどちらが改ざんしたかを公証人Nが特定することができる。

【0092】以上説明したモデルのうち、第2および第3のモデルでは、ユーザAとユーザBの間で取り引き情報がやりとりされるので、送信者の電子署名を検証するために公開鍵を用いる必要がある。したがって、RSA(Rivest-Shamir-Adleman)暗号のような公開鍵システムが前提となる。

【0093】これに対して、第1および第4のモデルでは、ユーザAと公証人Nの間またはユーザBと公証人Nの間で取り引き情報がやりとりされ、ユーザAとユーザBの間では取り引き情報がやりとりされない。この場合、DES(Data Encryption Standard)暗号のような秘密鍵システムでも、身元保証サービスを実現することが可能である。ただし、公証人NはユーザAとユーザBの秘密鍵を知っている必要がある。

【0094】次に、図11から図19までを参照しながら、取り引き保証サービスの実施形態について説明する。ユーザAとユーザBが取り引きした事実を保証するには、以下のようなサービス要件が考えられる。

(1) ユーザBと取り引きした事実をユーザAが第3者Cに対して証明するために、取り引き文書にユーザBの電子署名を付けた情報に対して、公証人Nの電子署名を付ける。

(2) ユーザAと取り引きした事実をユーザBが第3者Cに対して証明するために、取り引き文書にユーザAの電子署名を付けた情報に対して、公証人Nの電子署名を付ける。

(3) ユーザBと取り引きした事実をユーザAが否定できないように、取り引き文書にユーザAの電子署名を付

けた情報に対する公証人Nの電子署名を、公証人NとユーザBが保持する。

〈4〉ユーザAと取り引きした事実をユーザBが否定できないように、取り引き文書にユーザBの電子署名を付けた情報に対する公証人Nの電子署名を、公証人NとユーザAが保持する。

【0095】以上の要件を満たすためには、取り引き文書にユーザAとユーザBの電子署名を付けた情報に対する公証人Nの電子署名を、最終的にユーザA、B、および公証人Nが共有すればよい。図11においては、取り引き文書M、ユーザAの電子署名SA(M)、およびユーザBの電子署名SB(M)を連結した情報に対する公証人Nの電子署名SN(M, SA(M), SB(M))が、ユーザA、B、および公証人Nにより共有されている。

【0096】この取り引き保証サービスは、上述の内容保証サービスと密接に関係しているため、内容保証サービスの実施形態を元にして実現される。図7、8、9、10に示した4つの基本モデルに対応して、取り引き保証サービスの基本モデルは、図12、13、14、15に示す4つのモデルになる。

【0097】これらのモデルにおいては、内容保証サービスと同様に、図6のような取り引き文書Mが用いられ、ユーザA、B、および公証人Nの間でやりとりされる情報には発信者の電子署名が付いている。受信者はその電子署名を検証することで、発信者の身元を確認することができる。したがって、これらのモデルは、身元保証サービス、日時保証サービス、一意性保証サービス、および内容保証サービスを含んでいる。

【0098】図12は、取り引き保証サービスの第1のモデルを示している。第1のモデルでは、ユーザA、Bがオンラインまたはオフラインで取り引き内容Pを交換した後、それぞれが公証装置11に対して取り引き情報を送付する。図12における処理の流れは、次のようになる。

【0099】P40：ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P40'：ユーザBの端末12Bが、公証装置11から日時情報TとトランザクションIDを取得する。

【0100】P41：端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それをを用いて取り引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を公証装置11に送信する。

【0101】P41'：端末12Bが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書M'を作成する。次に、ユーザBの秘密鍵SBを取り出し、それをを用いて取り引き文書M'に対する電

子署名SB(M')を作成する。そして、データ{M', SB(M')}を公証装置11に送信する。

【0102】P42：公証装置11が、データ{M, SA(M)}とデータ{M', SB(M')}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M')を検証する。ここで、SA(M)またはSB(M')が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

【0103】次に、公証装置11は、取り引き文書MとM'が同一かどうかを確認する。また、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。取り引き文書MとM'が一致しない場合、あるいは、日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0104】次に、公証装置11は、取り引き文書M、電子署名SA(M)、SB(M')を連結して、データ{M, SA(M), SB(M')}を作成する。次に、公証人Nの秘密鍵SNを取り出し、それをを用いてデータ{M, SA(M), SB(M')}に対する電子署名SN(M, SA(M), SB(M'))を作成する。そして、データ{M, SA(M), SB(M'), SN(M, SA(M), SB(M'))}を保存する。

【0105】P43：公証装置11が、データ{M, SA(M), SB(M'), SN(M, SA(M), SB(M'))}を端末12Aに送信する。

P43'：公証装置11が、データ{M, SA(M), SB(M'), SN(M, SA(M), SB(M'))}を端末12Bに送信する。

【0106】P44：端末12Aが、データ{M, SA(M), SB(M'), SN(M, SA(M), SB(M'))}を受信する。そして、公証人Nの公開鍵PNを取り出し、それをを用いて電子署名SN(M, SA(M), SB(M'))を検証する。また、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M')を検証する。ここで、SN(M, SA(M), SB(M'))、SA(M)、SB(M')のいずれかが正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。

【0107】次に、端末12Aは、公証装置11から受け取った取り引き文書Mと端末12Aが作成した取り引き文書Mが同一かどうかを確認する。受け取った取り引き文書Mが正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それが正しければ、データ{M, SA(M), SB(M'), SN(M, SA(M), SB(M'))}を保存して、処理を終了する。

【0108】P44'：端末12Bが、データ{M, S

A (M), SB (M'), SN (M, SA (M), SB (M'))))を受信する。そして、公証人Nの公開鍵PNを取り出し、それを用いて電子署名SN (M, SA (M), SB (M'))))を検証する。また、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA (M)を検証し、公開鍵PBでSB (M')を検証する。ここで、SN (M, SA (M), SB (M'))))、SA (M)、SB (M')のいずれかが正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0109】次に、端末12Bは、公証装置11から受け取った取り引き文書M'と端末12Bが作成した取り引き文書M'が同一かどうかを確認する。受け取った取り引き文書M'が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。それが正しければ、データ {M, SA (M), SB (M'), SN (M, SA (M), SB (M'))))}を保存して、処理を終了する。

【0110】図13は、取り引き保証サービスの第2のモデルを示している。第2のモデルでは、ユーザA、Bがオンラインまたはオフラインで取り引き内容Pを交換した後、ユーザAのみが公証装置11に対して取り引き情報を送付する。図13における処理の流れは、次のようになる。

【0111】P50: ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P51: 端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA (M)を作成する。そして、データ {M, SA (M)}を端末12Bに送信する。

【0112】P52: 端末12Bが、データ {M, SA (M)}を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA (M)を検証する。ここで、SA (M)が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0113】次に、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB (M)を作成する。そして、データ {M, SA (M), SB (M)}を作成して、それを保存する。

【0114】P53: 端末12Bが、データ {M, SA (M), SB (M)}を端末12Aに送信する。

P54: 端末12Aが、データ {M, SA (M), SB (M)}を受信する。そして、ユーザBの公開鍵PBを取り出し、それを用いてSB (M)を検証する。ここで、SB (M)が正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それが正しければ、データ {M, SA (M), SB (M)}を保

存する。

【0115】P55: 端末12Aが、データ {M, SA (M), SB (M)}を公証装置11に送信する。

P56: 公証装置11が、データ {M, SA (M), SB (M)}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA (M)を検証し、公開鍵PBでSB (M)を検証する。ここで、SA (M)またはSB (M)が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

10 【0116】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0117】次に、公証装置11は、公証人Nの秘密鍵SNを取り出し、それを用いてデータ {M, SA (M), SB (M)}に対する電子署名SN (M, SA (M), SB (M))を作成する。そして、データ {M, SA (M), SB (M), SN (M, SA (M), SB (M))}を作成し、それを保存する。

【0118】P57: 公証装置11が、電子署名SN (M, SA (M), SB (M))を端末12Aに送信する。

P57': 公証装置11が、電子署名SN (M, SA (M), SB (M))を端末12Bに送信する。

30 【0119】P58: 端末12Aが、電子署名SN (M, SA (M), SB (M))を受信する。そして、公証人Nの公開鍵PNを取り出し、それを用いてSN (M, SA (M), SB (M))を検証する。ここで、SN (M, SA (M), SB (M))が正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それが正しければ、電子署名SN (M, SA (M), SB (M))を保存して、処理を終了する。

【0120】P58': 端末12Bが、電子署名SN (M, SA (M), SB (M))を受信する。そして、公証人Nの公開鍵PNを取り出し、それを用いてSN (M, SA (M), SB (M))を検証する。ここで、SN (M, SA (M), SB (M))が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。それが正しければ、電子署名SN (M, SA (M), SB (M))を保存して、処理を終了する。

【0121】図14は、取り引き保証サービスの第3のモデルを示している。第3のモデルでは、ユーザA、Bがオンラインまたはオフラインで取り引き内容Pを交換した後、ユーザBのみが公証装置11に対して取り引き情報を送付する。図14における処理の流れは、次のようになる。

50 【0122】P60: ユーザAの端末12Aが、公証装

置11から日時情報TとトランザクションIDを取得する。

P61: 端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を端末12Bに送信する。

【0123】P62: 端末12Bが、データ{M, SA(M)}を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA(M)を検証する。ここで、SA(M)が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0124】次に、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB(M)を作成する。そして、データ{M, SA(M), SB(M)}を作成して、それを保存する。

【0125】P63: 端末12Bが、データ{M, SA(M), SB(M)}を公証装置11に送信する。

P64: 公証装置11が、データ{M, SA(M), SB(M)}を受信する。そして、ユーザA、Bの公開鍵PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証する。ここで、SA(M)またはSB(M)が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

【0126】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0127】次に、公証装置11は、公証人Nの秘密鍵SNを取り出し、それを用いてデータ{M, SA(M), SB(M)}に対する電子署名SN(M, SA(M), SB(M))を作成する。そして、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を作成し、それを保存する。

【0128】P65: 公証装置11が、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を端末12Aに送信する。

P65': 公証装置11が、電子署名SN(M, SA(M), SB(M))を端末12Bに送信する。

【0129】P66: 端末12Aが、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を受信する。そして、ユーザA、B、公証人Nの公開鍵PA、PB、PNを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証し、公開鍵PNでSN(M, SA(M), SB(M))を検証する。

【0130】ここで、SA(M)、SB(M)、SN(M, SA(M), SB(M))のいずれかが正しくな

ければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それらが正しければ、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を保存して、処理を終了する。

【0131】P66': 端末12Bが、電子署名SN(M, SA(M), SB(M))を受信する。そして、公証人Nの公開鍵PNを取り出し、それを用いてSN(M, SA(M), SB(M))を検証する。ここで、SN(M, SA(M), SB(M))が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。それが正しければ、電子署名SN(M, SA(M), SB(M))を保存して、処理を終了する。

【0132】図15は、取り引き保証サービスの第4のモデルを示している。第4のモデルでは、公証装置11がユーザAとユーザBの取り引きを仲介する。図15における処理の流れは、次のようになる。

【0133】P70: ユーザAの端末12Aが、公証装置11から日時情報TとトランザクションIDを取得する。

P71: 端末12Aが、日時情報TとトランザクションIDと取り引き内容Pを連結して、取り引き文書Mを作成する。次に、ユーザAの秘密鍵SAを取り出し、それを用いて取り引き文書Mに対する電子署名SA(M)を作成する。そして、データ{M, SA(M)}を公証装置11に送信する。

【0134】P72: 公証装置11が、データ{M, SA(M)}を受信する。そして、ユーザAの公開鍵PAを取り出し、それを用いてSA(M)を検証する。ここで、SA(M)が正しくなければ、端末12Aにエラー通知を行って処理を終了する。それが正しければ、データ{M, SA(M)}を端末12Bに送信する。

【0135】P73: 端末12Bが、データ{M, SA(M)}を受信する。ユーザBは、受け取った取り引き文書Mの中の取り引き内容Pを見て、その取り引きに応じられない場合は、その旨を端末12Aに通知し、端末12Bの処理を終了させる。また、その取り引きに応じる場合は、端末12Bに処理の続行を指示する。

【0136】次に、端末12Bは、ユーザAの公開鍵PAを取り出し、それを用いてSA(M)を検証する。ここで、SA(M)が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。

【0137】次に、端末12Bは、ユーザBの秘密鍵SBを取り出し、それを用いて取り引き文書Mに対する電子署名SB(M)を作成する。そして、データ{M, SA(M), SB(M)}を作成して、それを保存する。

【0138】P74: 端末12Bが、データ{M, SA(M), SB(M)}を公証装置11に送信する。

P75: 公証装置11が、データ{M, SA(M), SB(M)}を受信する。そして、ユーザA、Bの公開鍵

PA、PBを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証する。ここで、SA(M)またはSB(M)が正しくなければ、端末12A、12Bにエラー通知を行って処理を終了する。

【0139】次に、公証装置11は、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する。日時情報TまたはトランザクションIDが正しくない場合は、端末12A、12Bにエラー通知を行って処理を終了する。

【0140】次に、公証装置11は、公証人Nの秘密鍵SNを取り出し、それを用いてデータ{M, SA(M), SB(M)}に対する電子署名SN(M, SA(M), SB(M))を作成する。そして、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を作成し、それを保存する。

【0141】P76:公証装置11が、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を端末12Aに送信する。

P76':公証装置11が、電子署名SN(M, SA(M), SB(M))を端末12Bに送信する。

【0142】P77:端末12Aが、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を受信する。そして、ユーザA、B、公証人Nの公開鍵PA、PB、PNを取り出し、公開鍵PAでSA(M)を検証し、公開鍵PBでSB(M)を検証し、公開鍵PNでSN(M, SA(M), SB(M))を検証する。

【0143】ここで、SA(M)、SB(M)、SN(M, SA(M), SB(M))のいずれかが正しくなければ、公証装置11、端末12Bにエラー通知を行って処理を終了する。それらが正しければ、データ{M, SA(M), SB(M), SN(M, SA(M), SB(M))}を保存して、処理を終了する。

【0144】P77':端末12Bが、電子署名SN(M, SA(M), SB(M))を受信する。そして、公証人Nの公開鍵PNを取り出し、それを用いてSN(M, SA(M), SB(M))を検証する。ここで、SN(M, SA(M), SB(M))が正しくなければ、公証装置11、端末12Aにエラー通知を行って処理を終了する。それが正しければ、電子署名SN(M, SA(M), SB(M))を保存して、処理を終了する。

【0145】次に、図16から図19までのフローチャートを参照しながら、図12に示した取り引き保証サービスの第1のモデルにおける公証装置11、端末12A、12Bの処理について、再び説明する。

【0146】図16は、端末12Aの処理P40、P41、または端末12Bの処理P40'、P41'に対応するフローチャートである。図16において処理が開始されると、端末12A(または端末12B)は、まず公

証装置11からネットワーク13を介して、日時情報TとトランザクションIDを取得する(ステップS1)。

【0147】次に、日時情報TとトランザクションIDと取り引き内容Pを連結して、図6のような取り引き文書M(またはM')を作成する(ステップS2)。次に、ユーザの秘密鍵SA(またはSB)を取り出し(ステップS3)、それを用いて取り引き文書Mに対するユーザの電子署名SA(M)(またはSB(M'))を作成する(ステップS4)。

【0148】そして、取り引き文書M(またはM')とユーザの電子署名SA(M)(またはSB(M'))を、ネットワーク13を介して公証装置11に送信し(ステップS5)、処理を終了する。

【0149】図17、18は、公証装置11の処理P42、P43、P43'に対応するフローチャートである。図17において処理が開始されると、公証装置11は、まずネットワーク13を介して、ユーザAの端末12Aから取り引き文書Mと電子署名SA(M)を受信し、ユーザBの端末12Bから取り引き文書M'と電子署名SB(M')を受信する(ステップS11)。

【0150】次に、ユーザA、Bの公開鍵PA、PBを取り出し(ステップS12)、公開鍵PAでSA(M)を検証して(ステップS13)、SA(M)が有効かどうかを判定する(ステップS14)。ここでは、電子署名SA(M)を公開鍵PAで復号化したデータが取り引き文書Mと同一とみなされるとき、SA(M)が有効となる。もし、SA(M)が有効でなければ、端末12A、12Bにエラー通知を行って(ステップS19)、処理を終了する。

【0151】SA(M)が有効であれば、次に、公開鍵PBでSB(M')を検証して(ステップS15)、SB(M')が有効かどうかを判定する(ステップS16)。ここで、SB(M')が有効でなければ、端末12A、12Bにエラー通知を行って(ステップS19)、処理を終了する。

【0152】SB(M')が有効であれば、次に、取り引き文書MとM'が一致するかどうかを確認する(ステップS17)。これらが一致しなければ、端末12A、12Bにエラー通知を行って(ステップS19)、処理を終了する。

【0153】取り引き文書MとM'が一致すれば、次に、取り引き文書Mの中の日時情報TとトランザクションIDが、発行したものと一致するかどうかを確認する(ステップS18)。日時情報TまたはトランザクションIDが正しくなければ、端末12A、12Bにエラー通知を行って(ステップS19)、処理を終了する。

【0154】これらが正しければ、次に、取り引き文書M、電子署名SA(M)、SB(M')を連結して、データ{M, SA(M), SB(M')}を作成する(図18、ステップS20)。

【0155】次に、公証人Nの秘密鍵SNを取り出し（ステップS21）、それを用いてデータ[M, SA(M), SB(M')]に対する公証人Nの電子署名SN(M, SA(M), SB(M'))を作成する（ステップS22）。そして、取り引き文書M、電子署名SA(M)、SB(M')、SN(M, SA(M), SB(M'))を保存する（ステップS23）。

【0156】そして、これらのデータM、SA(M)、SB(M')、SN(M, SA(M), SB(M'))を、ネットワーク13を介して端末12A、12Bに送信して（ステップS24）、処理を終了する。

【0157】図19は、端末12Aの処理P44、または端末12Bの処理P44'に対応するフローチャートである。図19において処理が開始されると、端末12A（または端末12B）は、まずネットワーク13を介して、公証装置11から取り引き文書M、電子署名SA(M)、SB(M')、SN(M, SA(M), SB(M'))を受信する（ステップS31）。

【0158】次に、公証人Nの公開鍵PNを取り出し（ステップS32）、それを用いて公証人Nの電子署名SN(M, SA(M), SB(M'))を検証して（ステップS33）、それが有効かどうかを判定する（ステップS34）。ここでは、電子署名SN(M, SA(M), SB(M'))を公開鍵PNで復号化したデータが、データ[M, SA(M), SB(M')]と同一とみなされるとき、SN(M, SA(M), SB(M'))が有効となる。

【0159】もし、公証人Nの電子署名が有効でなければ、公証装置11、端末12B（または端末12A）にエラー通知を行って（ステップS43）、処理を終了する。公証人Nの電子署名が有効であれば、次に、取り引き相手であるユーザB（またはユーザA）の公開鍵PB（またはPA）を取り出し（ステップS35）、それを用いて相手の電子署名SB(M')（またはSA(M)）を検証して（ステップS36）、それが有効かどうかを判定する（ステップS37）。相手の電子署名が有効でなければ、公証装置11、端末12B（または端末12A）にエラー通知を行って（ステップS43）、処理を終了する。

【0160】相手の電子署名が有効であれば、次に、当方の公開鍵PA（またはPB）を取り出し（ステップS38）、それを用いて当方の電子署名SA(M)（またはSB(M'））を検証して（ステップS39）、それが有効かどうかを判定する（ステップS40）。当方の電子署名が有効でなければ、公証装置11、端末12B（または端末12A）にエラー通知を行って（ステップS43）、処理を終了する。

【0161】当方の電子署名が有効であれば、次に、公証装置11から受け取った取り引き文書Mが正しいかどうかを確認する（ステップS41）。ここでは、受け取

った取り引き文書Mが、当方が作成した取り引き文書M（またはM'）と同一であれば、それが正しいと判定する。受け取った取り引き文書Mが正しくなければ、公証装置11、端末12B（または端末12A）にエラー通知を行って（ステップS43）、処理を終了する。

【0162】受け取った取り引き文書Mが正しければ、取り引き文書M、電子署名SA(M)、SB(M')、SN(M, SA(M), SB(M'))を保存して（ステップS42）、処理を終了する。

【0163】こうして、図16、17、18、19に示した一連の処理により、取り引き文書、ユーザAの電子署名、ユーザBの電子署名、および公証人Nの電子署名が、ユーザA、B、公証人Nの間で共有されることになる。取り引き保証サービスの他のモデル、および内容保証サービスについても、同様のフローチャートを作成することが可能である。

【0164】公証装置11は、取り引き内容を確認したい任意のユーザの端末から取り引き情報の参照要求を受け取ると、保存されている取り引き文書を、公証人Nの電子署名とともに要求元の端末に送り返す。こうして、要求者は、公証人Nにより保証された取り引き文書の内容を参照することができる。

【0165】以上、取り引き公証システムにおけるサービスとして、身元保証サービス、日時保証サービス、一意性保証サービス、配達保証サービス、内容保証サービス、および取り引き保証サービスについて述べたが、取り引き公証システムの望ましい実施形態は、図12から図15に示した4つの基本モデルから成ると考えられる。また、これらを元にした取り引き公証システムの応用モデルとして、暗号化モデル、多重署名モデル、および双方向モデルがある。

【0166】暗号化モデルとは、各基本モデルにおいてネットワーク上でやりとりされる情報全体を、受信者の公開鍵で暗号化して送信する実施形態である。受信者は、自分の秘密鍵で情報を復号化した後に、基本モデルと同様の処理を行う。このように情報を暗号化することで、ユーザA、Bと公証人N以外の者に取り引き情報を盗用される可能性が低くなる。

【0167】また、基本モデルでは、ユーザA、Bが、取り引き文書Mを元に電子署名SA(M)、SB(M)を作成していた。多重署名モデルでは、取り引き文書Mと一方のユーザの電子署名とを連結した情報を元にして、もう一方のユーザが電子署名を作成する。例えば、ユーザAが先に電子署名SA(M)を作成した場合、ユーザBは、取り引き文書Mと電子署名SA(M)に対する電子署名SB(M, SA(M))を作成する。公証人Nは、さらに電子署名SB(M, SA(M))と取り引き文書Mを連結して、電子署名SN(SB(M, SA(M)))を作成することになる。

【0168】この多重署名モデルによれば、ユーザA、

Bのどちらが先に取り引き文書Mを承認したのかを明らかにすることができる。また、この多重署名モデルで作成された情報を受信者の公開鍵で暗号化した暗号化モデルも考えられる。

【0169】また、図13、14、15に示した第2、第3、第4のモデルでは、ユーザAが取り引き文書Mの第1発信者であり、ユーザBは受信した取り引き文書Mに基づいて応答するだけであった。

【0170】双方向モデルでは、これらの基本モデルにおいて、図12に示した第1のモデルと同様に、ユーザBからも取り引き文書M'を発信する。このように情報の流れを双方向にすることで、ユーザAとユーザBの立場が対等になる。この場合、公証装置11は、双方からの情報を検証して登録することになる。

【0171】4つの基本モデルとそれらから派生する応用モデルを列挙すると、取り引き公証システムのモデルのバリエーションは、図20に示すようになる。図20において、例えば“多重署名+暗号化”は、多重署名モデルと暗号化モデルを併用した複合モデルを表す。また、“○”は、対応する列の基本モデルと対応する行（第1行を除く）の応用モデルとの組合せが可能であることを表し、“×”は、その組合せが不可能であることを表す。

【0172】図20から分かるように、取り引き公証システムには23個のモデルがあることになる。さらに、取り引き公証システムの変形モデルとして、内容非開示モデルと合意署名モデルがある。

【0173】内容非開示モデルとは、公証人Nに取り引き内容を開示しないで、それを登録するモデルである。具体的には、各基本モデルおよび応用モデルにおいて、公証装置11への送信情報から、取り引き内容の平文Pを削除することで実現される。この場合でも、ユーザA、Bの作成した電子署名は公証装置11に送付されるので、公証装置11はこれを検証／登録することができる。

【0174】また、合意署名モデルとは、保存する取り引き情報にユーザA、B、公証人N以外の合意者の電子署名を添付するモデルである。このモデルを採用することで、取り引きの当事者以外のユーザが、その取り引きの事実や内容に承認を与えたことを証明することが可能になる。

【0175】図21は、このような合意署名を付加した共有情報の一例を示している。図21においては、取り引き文書Mに対して、ユーザA、Bの電子署名SA(M)、SB(M)以外に、合意者であるユーザC、D、・・・の電子署名SC(M)、SD(M)、・・・も付加され、それらを連結した情報を元に公証人Nの電子署名SN(SA(M), SB(M), SC(M), SD(M), ...)が作成されている。

【0176】このような合意署名モデルにおいて、ユー

ザC、D等が取り引きの当事者である場合は、取り引き公証システムは、自動的に3以上の当事者間の取り引きに関する事項を証明することになる。

【0177】

【発明の効果】本発明によれば、複数の情報処理装置を互いに接続したネットワーク環境において、ユーザ間で行われる取り引きの内容、日時、取り引き相手の身元等の取り引きに関する事項を、第3者が客観的に証明することができる。したがって、ネットワーク環境における取り引きの安全性が自動的に保証される。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】ネットワーク上での商取り引き環境を示す図である。

【図3】取り引き公証システムを示す図である。

【図4】情報処理装置の構成図である。

【図5】内容保証サービスにおける共有情報を示す図である。

【図6】取り引き文書の例を示す図である。

【図7】第1の内容保証サービスを示す図である。

【図8】第2の内容保証サービスを示す図である。

【図9】第3の内容保証サービスを示す図である。

【図10】第4の内容保証サービスを示す図である。

【図11】取り引き保証サービスにおける共有情報を示す図である。

【図12】第1の取り引き保証サービスを示す図である。

【図13】第2の取り引き保証サービスを示す図である。

【図14】第3の取り引き保証サービスを示す図である。

【図15】第4の取り引き保証サービスを示す図である。

【図16】ユーザ端末の第1の処理のフローチャートである。

【図17】公証装置の処理のフローチャート（その1）である。

【図18】公証装置の処理のフローチャート（その2）である。

【図19】ユーザ端末の第2の処理のフローチャートである。

【図20】取り引き公証システムのモデルを示す図である。

【図21】合意署名を付加した共有情報を示す図である。

【符号の説明】

1 取り引き証明装置

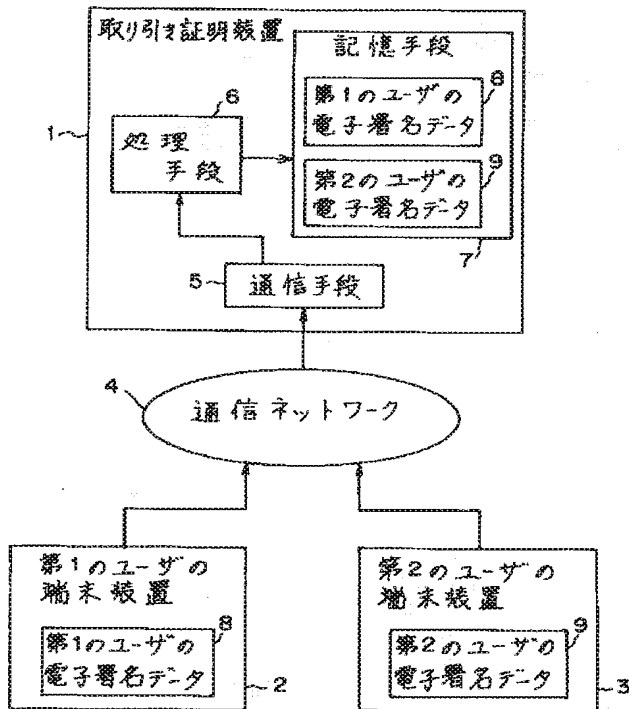
2、3、12A、12B、12C、12D ユーザの端末装置

4、13 通信ネットワーク

- 5 通信手段
- 6 処理手段
- 7 記憶手段
- 8、9 ユーザの電子署名データ
- 11 公証装置
- 21 CPU
- 22 メモリ
- 23 入力装置

【図1】

本発明の原理図



【図20】

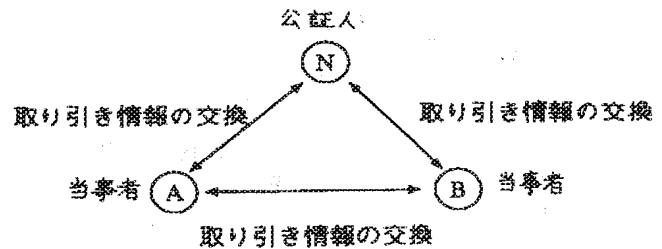
取引公証システムのモデルを示す図

	第1のモデル	第2のモデル	第3のモデル	第4のモデル
基本	○	○	○	○
暗号化	○	○	○	○
多重署名	×	○	○	○
多重署名+暗号化	×	○	○	○
双方向	×	○	○	○
双方向+暗号化	×	○	○	○
双方向+暗号化+多重署名	×	○	○	○

- 24 出力装置
- 25 外部記憶装置
- 26 媒体駆動装置
- 27 ネットワーク接続装置
- 28 バス
- 29 可搬記録媒体
- 30 データベース

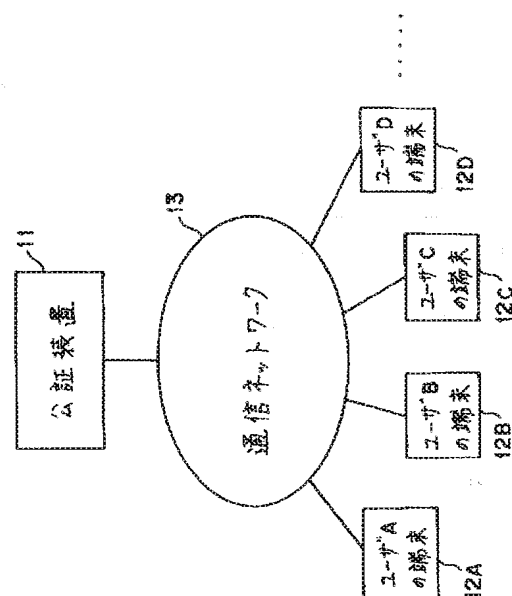
【図2】

ネットワーク上での商取引引き環境を示す図



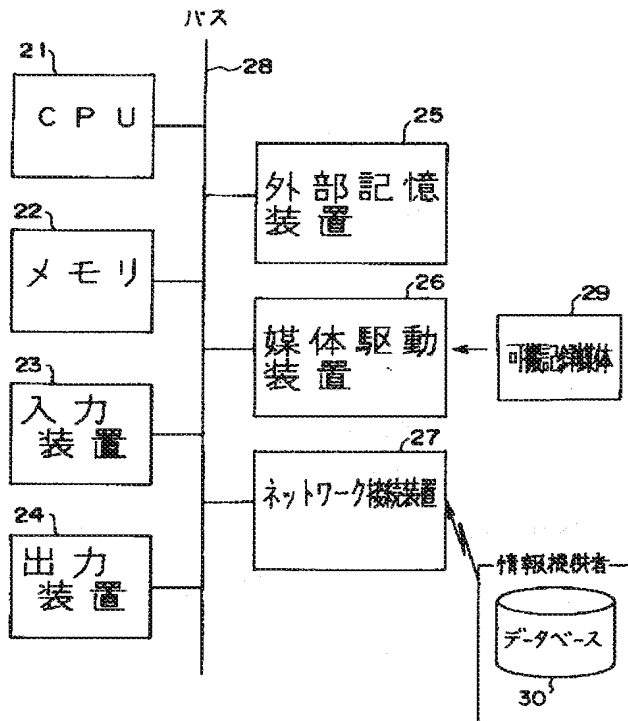
【図3】

取引公証システムを示す図



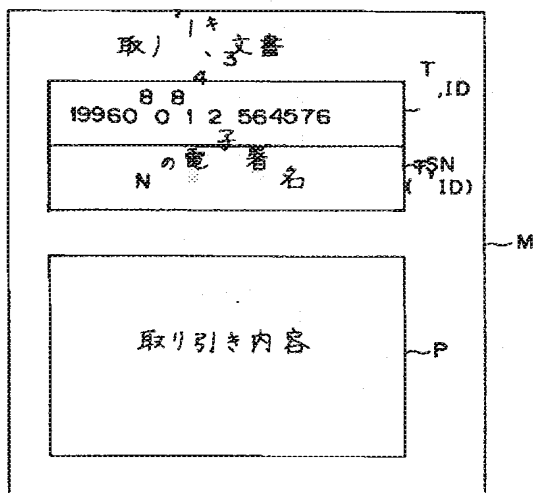
【図4】

情報処理装置の構成図



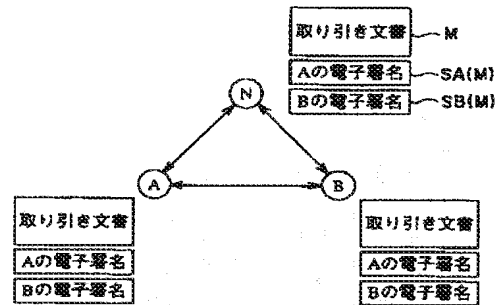
図

取り引き文書の例を示す図



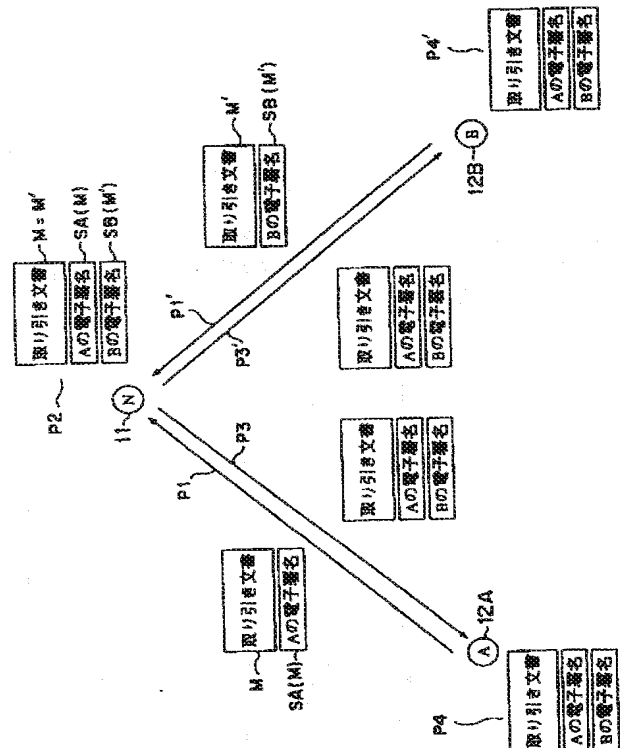
【図5】

内容保証サービスにおける共有情報を示す図



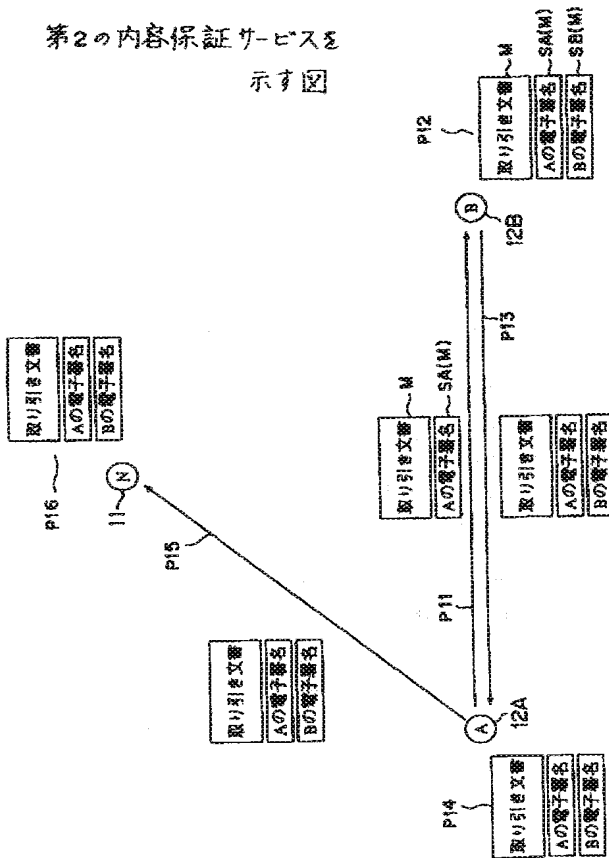
【図7】

第1の内容保証サービスを示す図



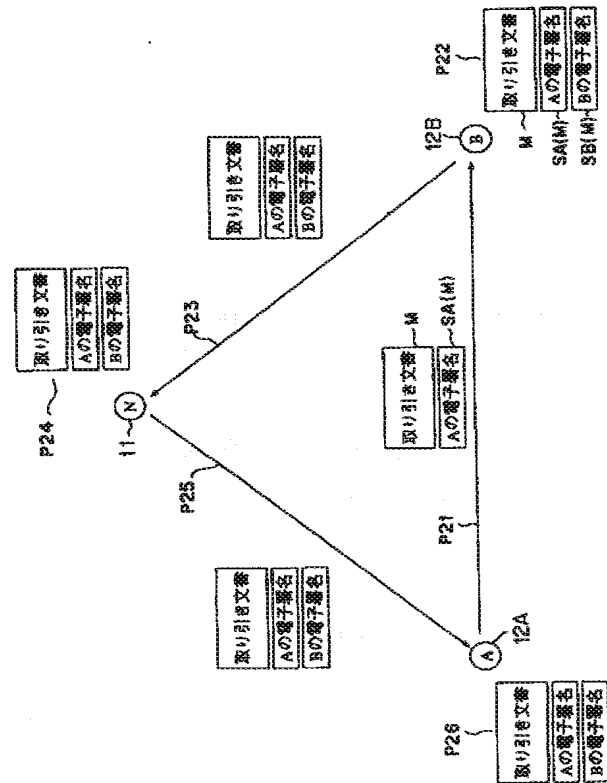
【図8】

第2の内容保証サービスを示す図



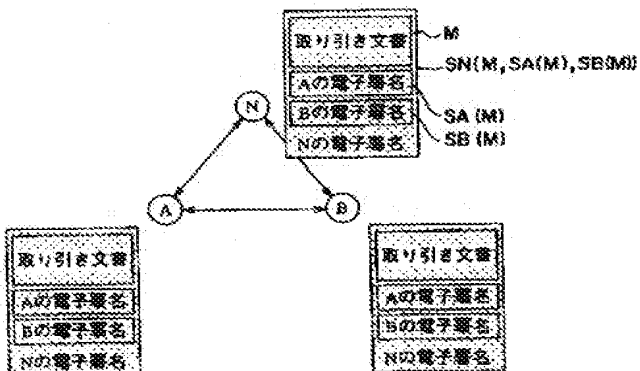
【図9】

第3の内容保証サービスを示す図



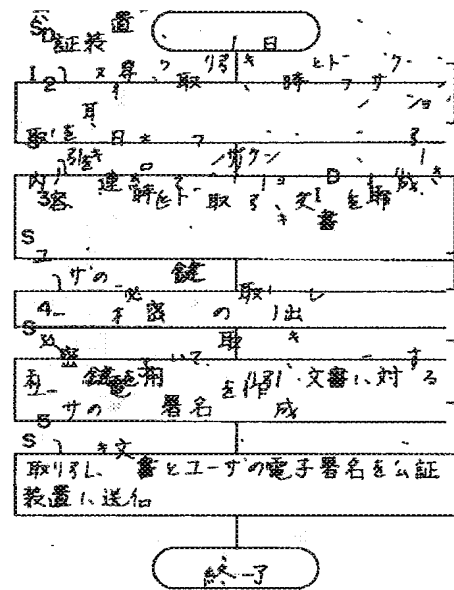
×11】

取り引き保証サービスにおける共有情報
を示す図

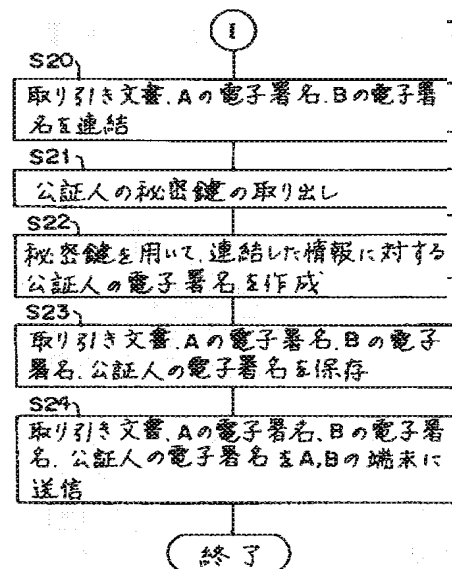


- 161

ユーザ端末の第1の処理のフローチャート

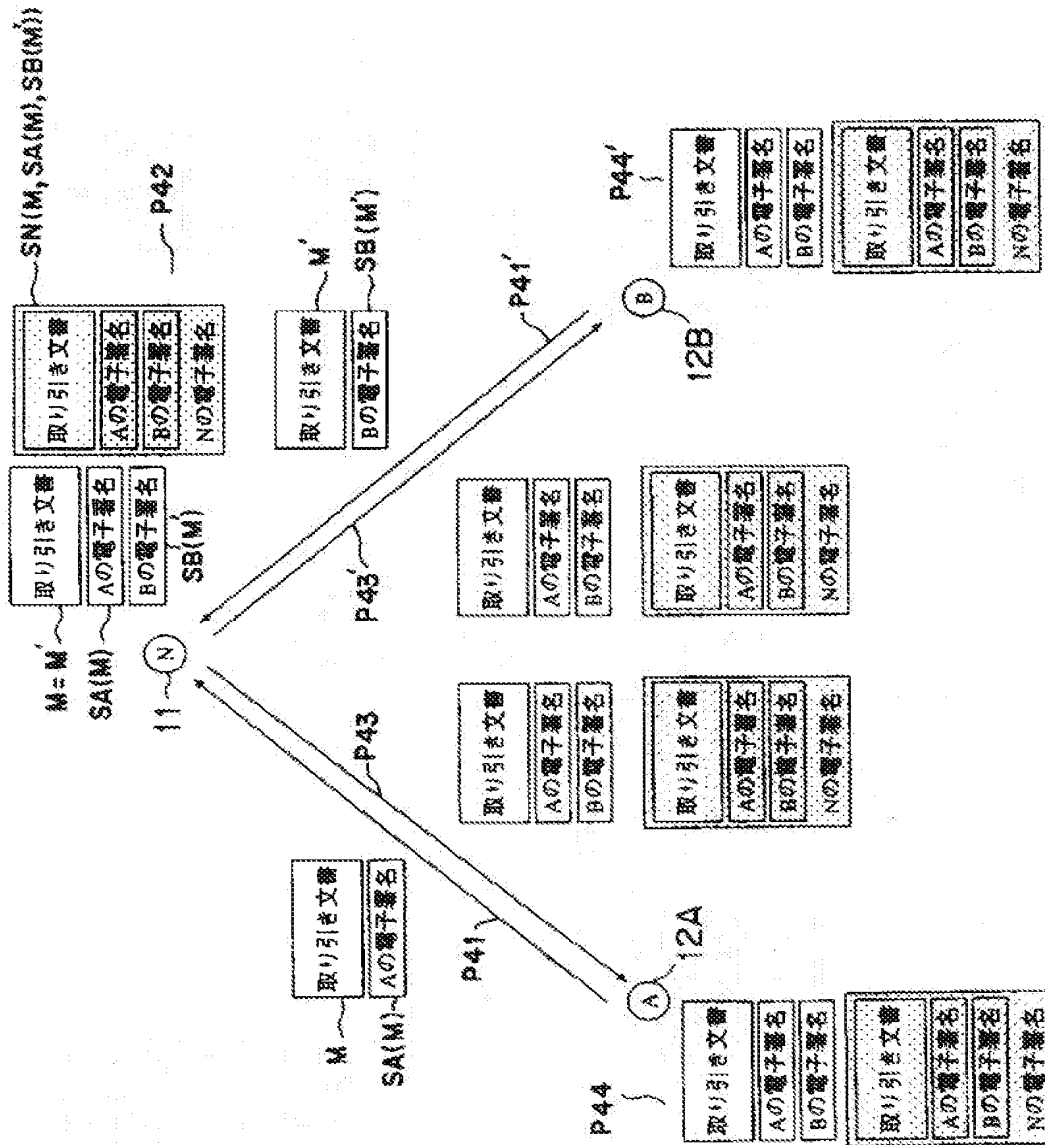


公証装置の処理のフローチャート(その2)



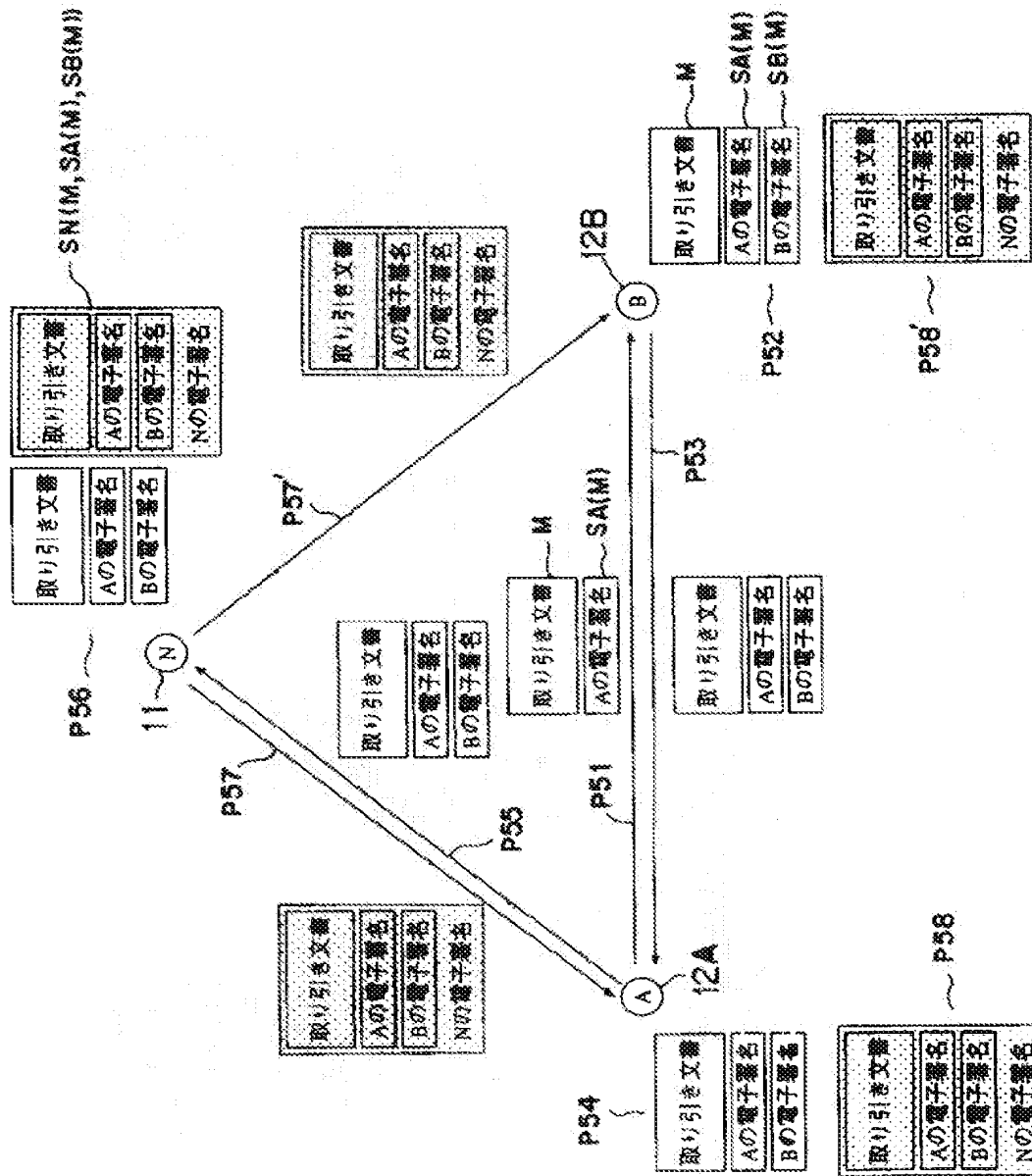
【図12】

第1の取り引き保証サービスの示す図

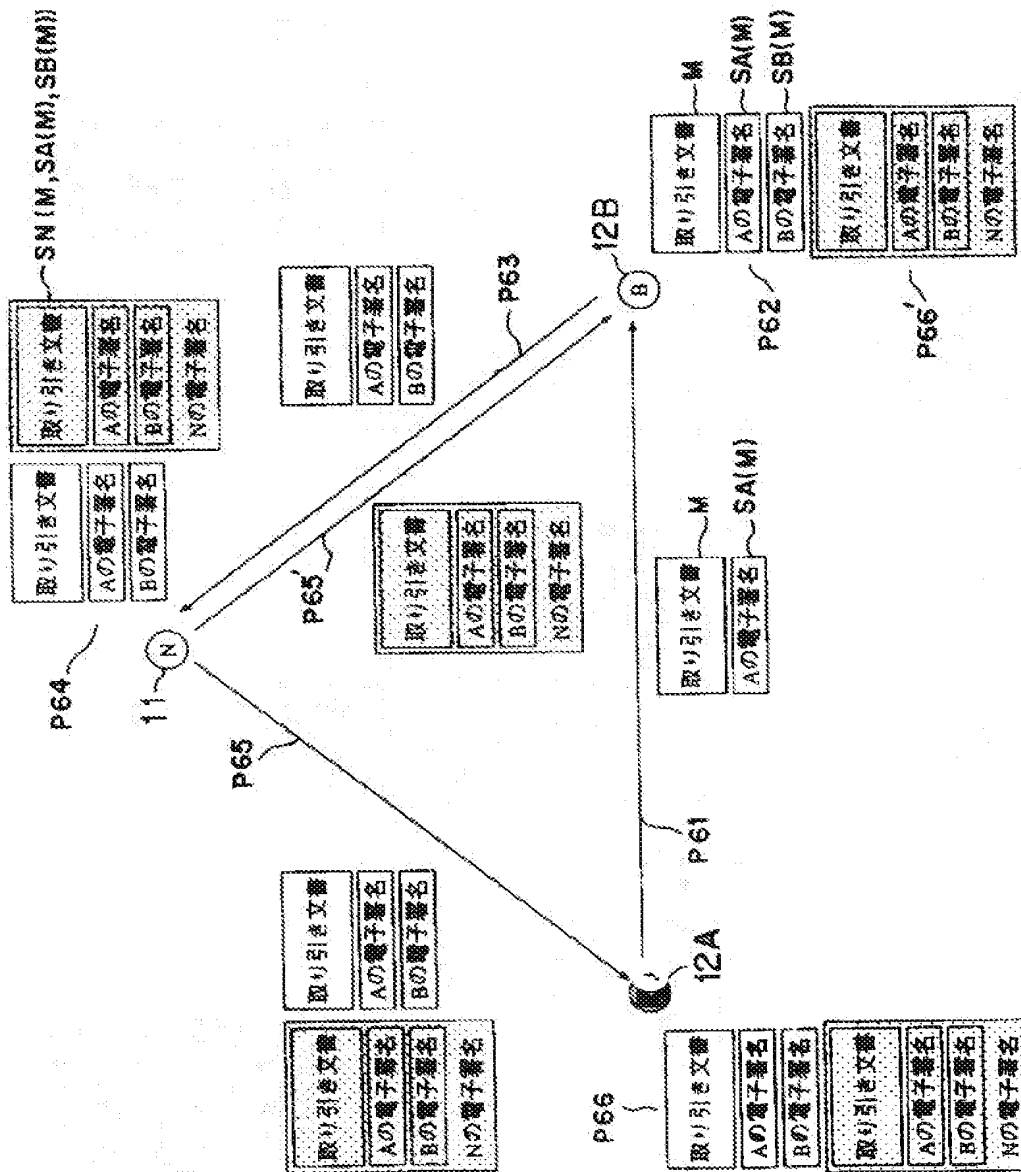


【図 3】

第2の取り引き保証サービスを示す図

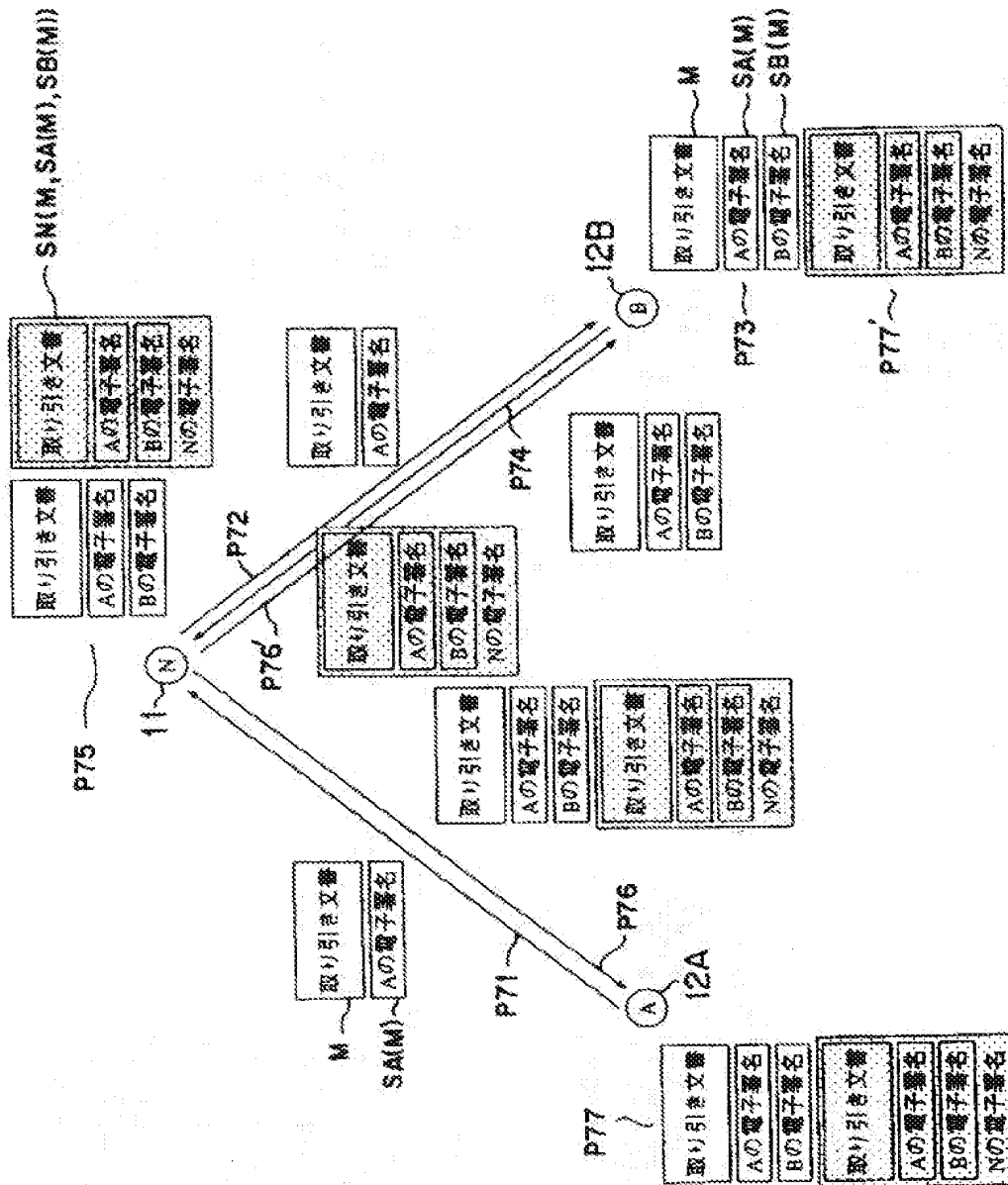


第3の取り引き保証サービスを示す図



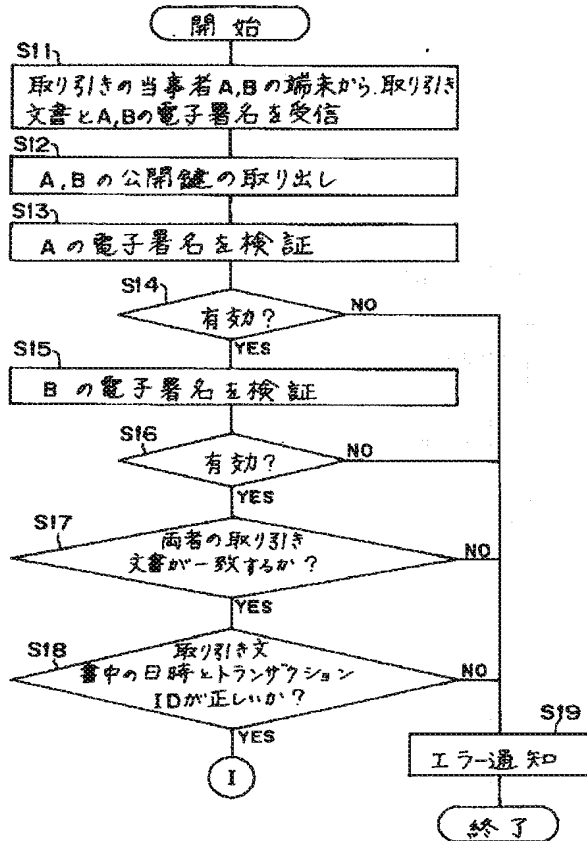
【図15】

第4の取り引き付^ロ証サービスを示す図



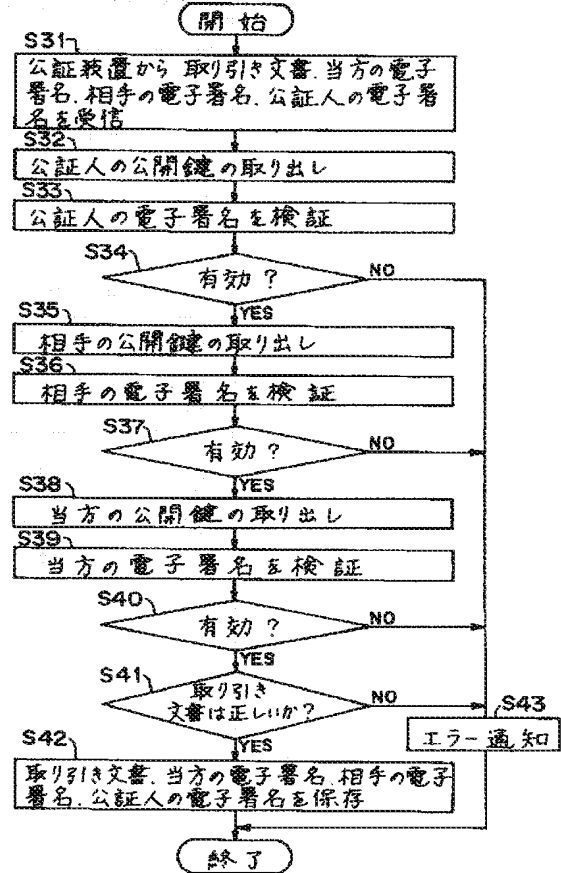
【図17】

公証装置の処理のフローチャート(その1)



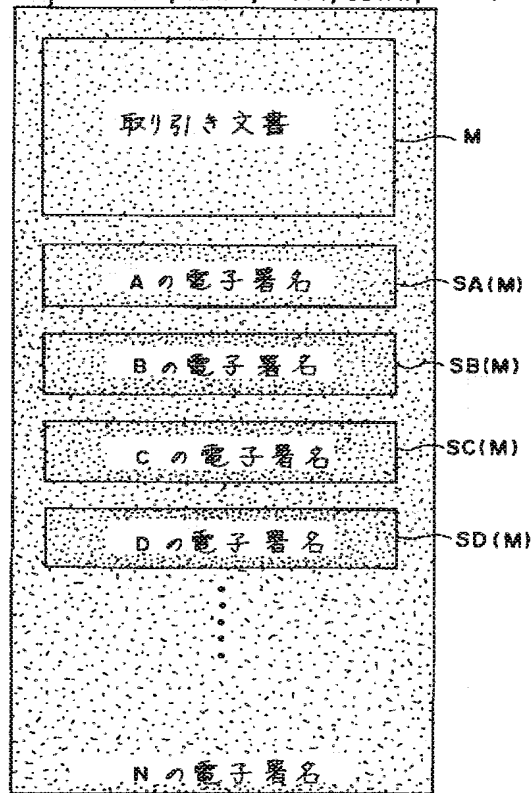
【図19】

ユーザ端末の第2の処理のフローチャート



【図21】

合意署名を付加した共有情報Eを示す図
 $SN(SA(M), SB(M), SC(M), SD(M), \dots)$



プロットヘン
 (72) 発明者 島 良一
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内

(72) 発明者 岩瀬 詔子
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72) 発明者 小野 越夫
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内